Práctica-(Tarea)

Recopilación Pasiva de Información utilizando Google Hacking y Shodan

Alejandro Garcia Burguillos

15/11/2024

Informe de Google Hacking y Exploración de Shodan

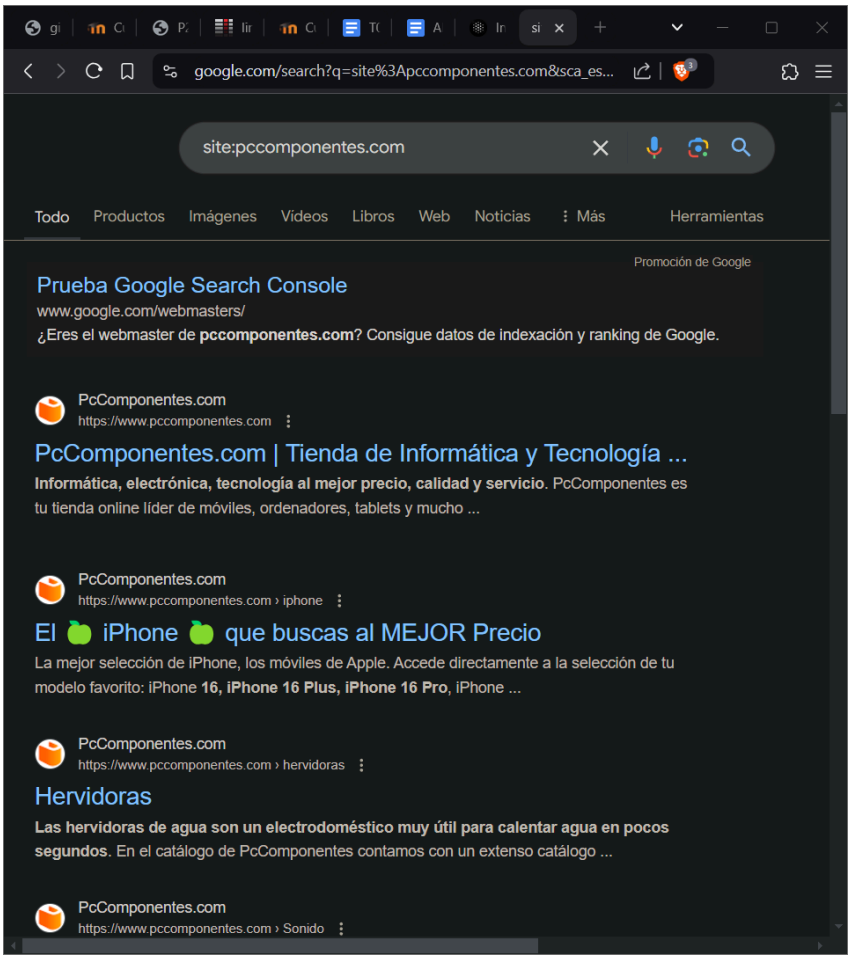
Parte 1: Google Hacking

Organización Seleccionada

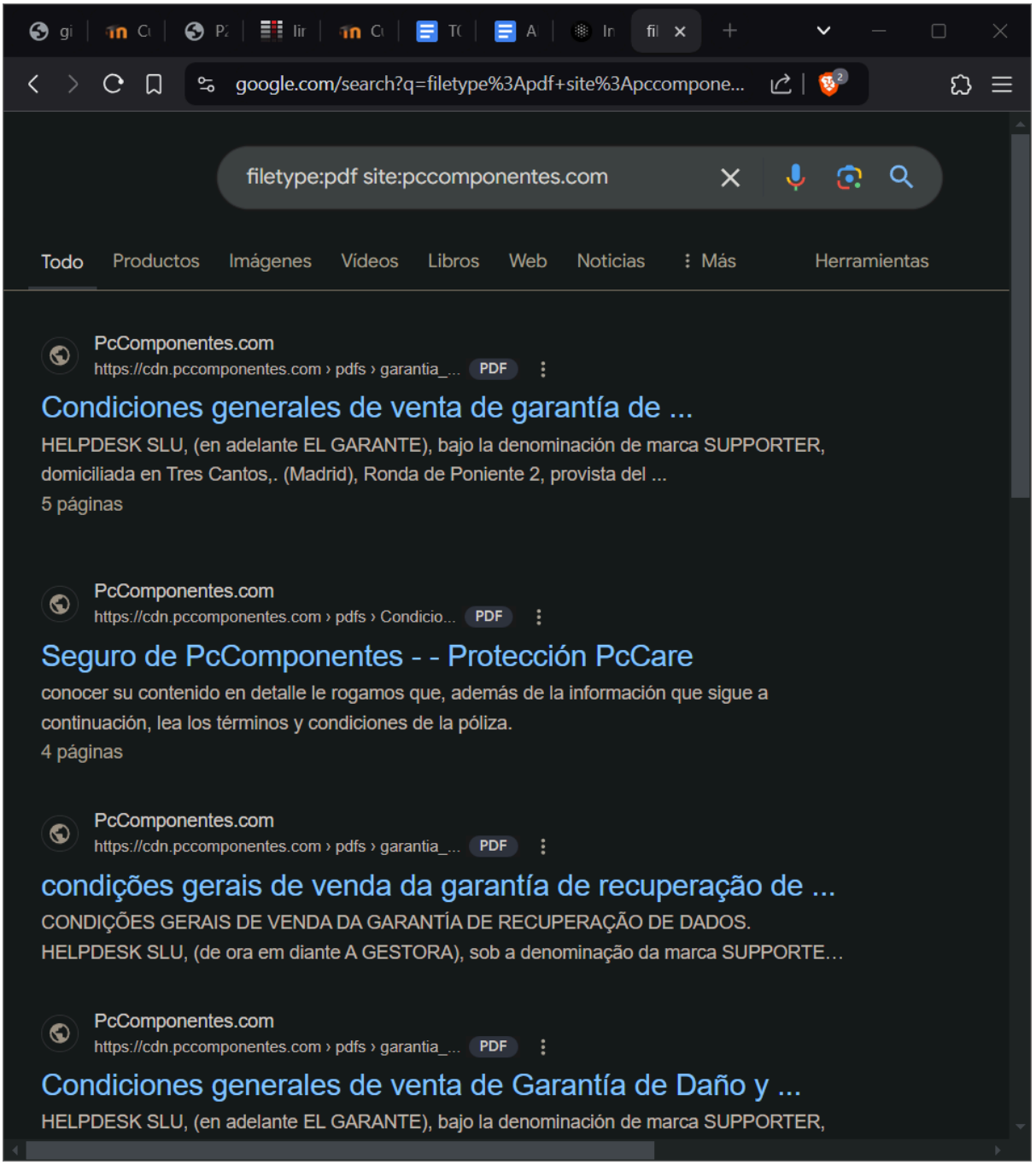
Para este ejercicio, he elegido pccomponentes empresa conocida de sobra aquí en España.

Búsquedas Avanzadas en Google

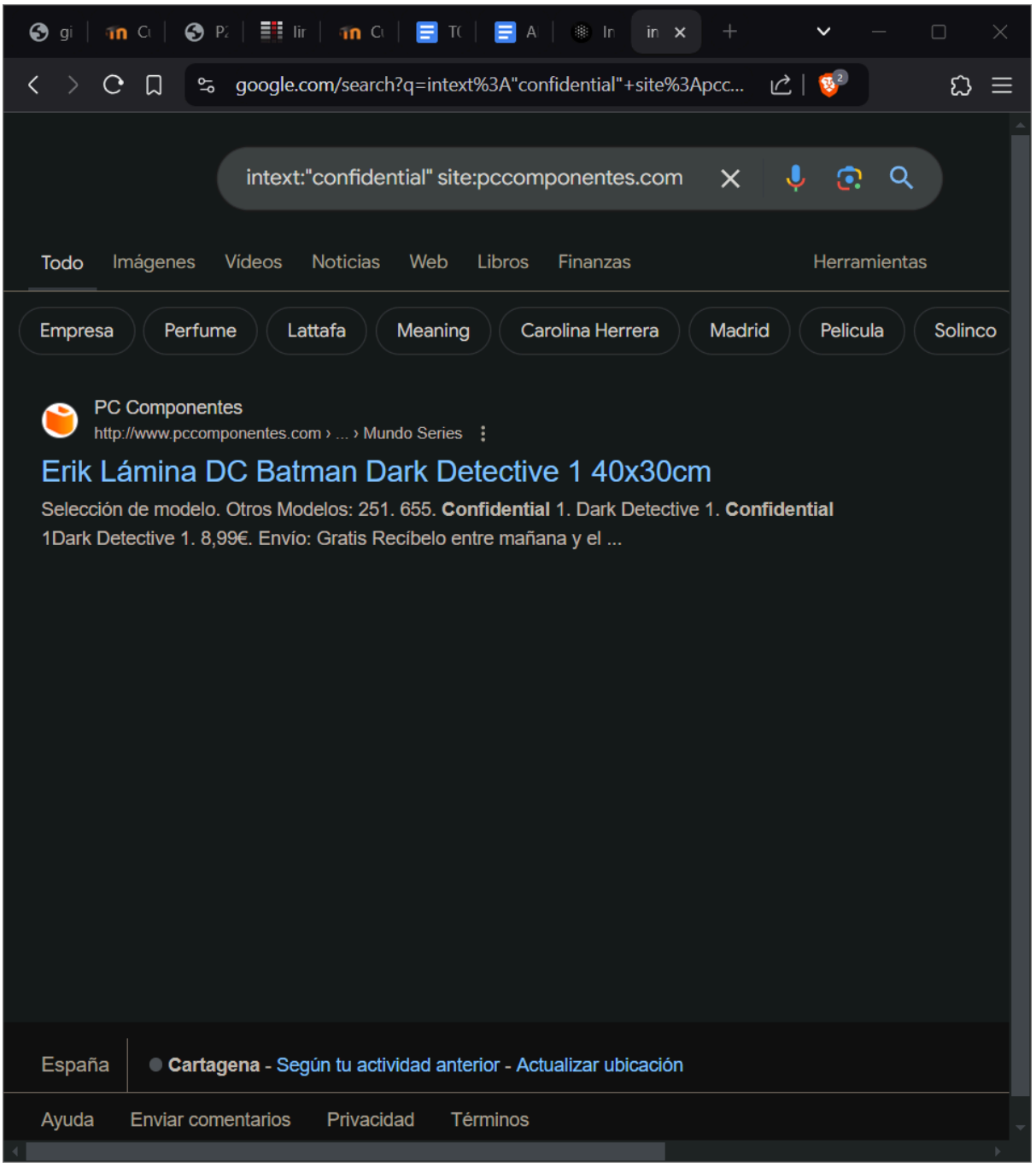
1. Búsqueda: **site:pccomponentes.com**
    - Resultados: Listado de páginas indexadas del sitio oficial de la organización.



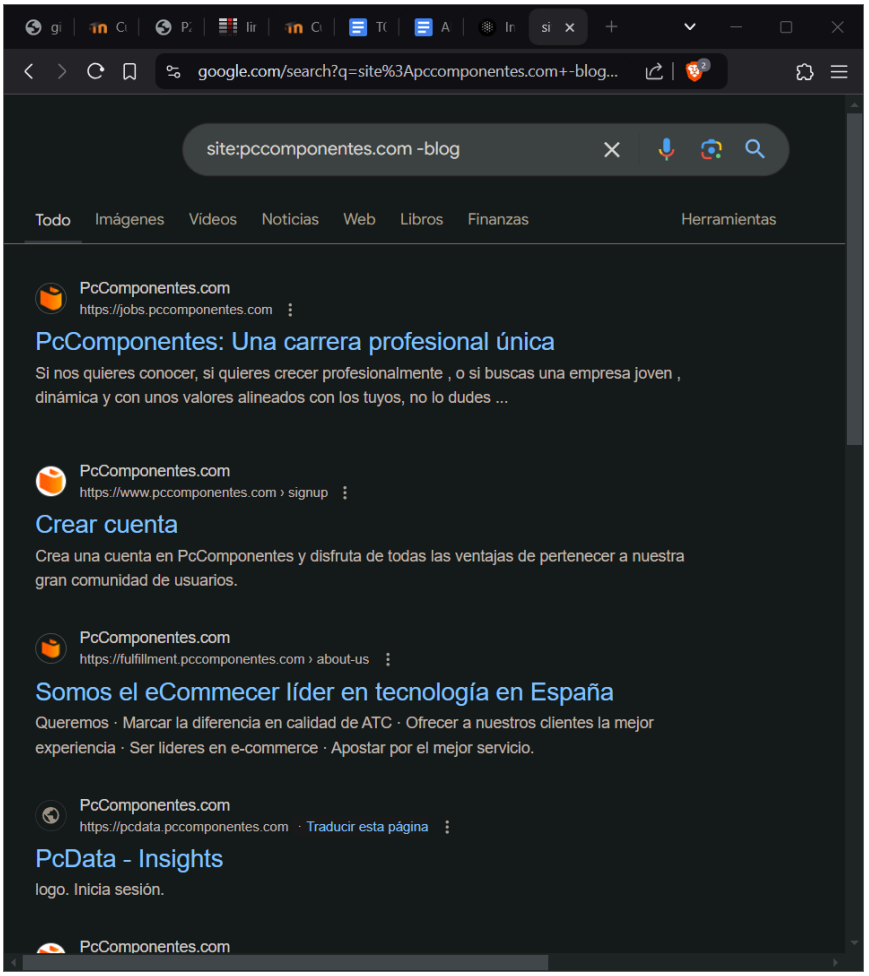
2. Búsqueda: **filetype:pdf site:pccomponentes.com**
    - Resultados: Documentos PDF disponibles en el sitio, incluyendo seguro y condiciones del servicio.



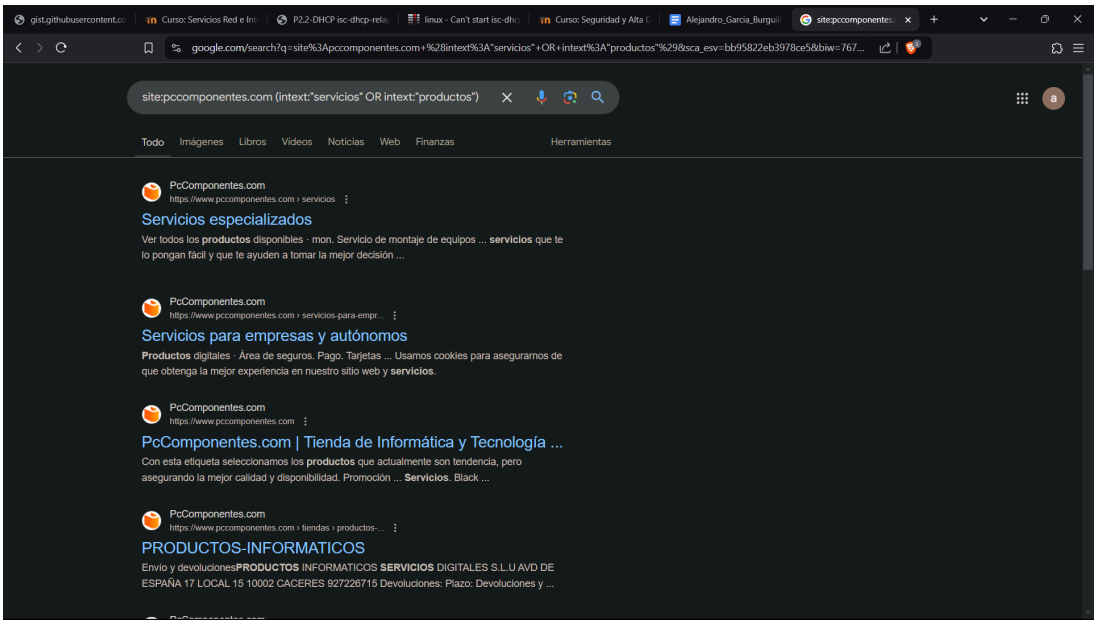
3. Búsqueda: **intext:”confidential” site:pccomponentes.com**
    - Resultados: Se encuentra una página pero no se encontraron documentos que contengan la palabra "confidential", lo que indica una buena práctica en la gestión de la información sensible.



4. Búsqueda: **site:pccomponentes.com -blog**
    - Resultados: Listado de páginas del sitio excluyendo la sección del blog.



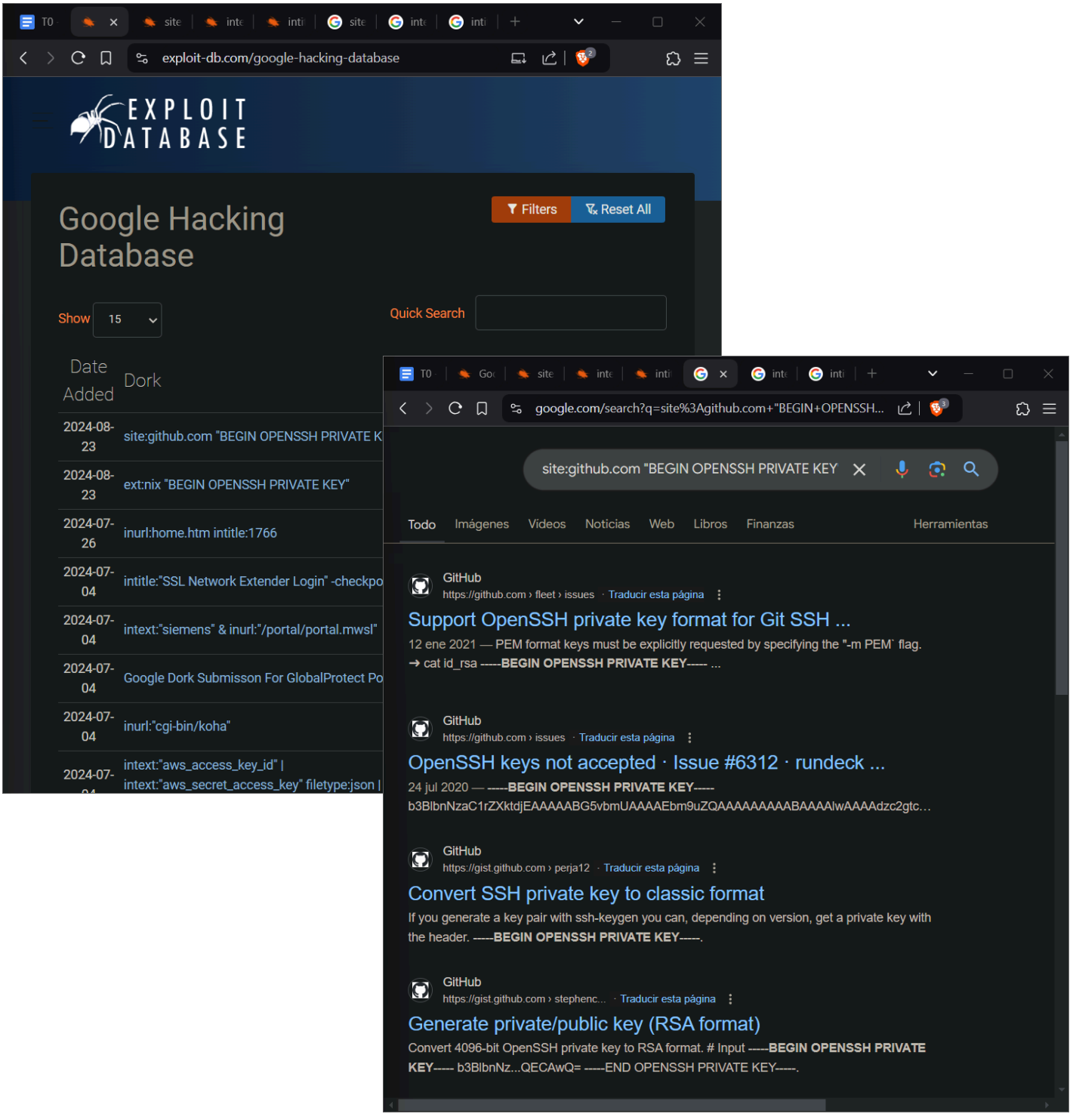
5. Búsqueda: site:pccomponentes.com (intext:”servicios” OR intext:”productos”
    - Resultados: Esta búsqueda busca páginas que contengan las palabras "servicios" o "productos" en el texto. Esto puede ayudar a identificar las ofertas específicas.



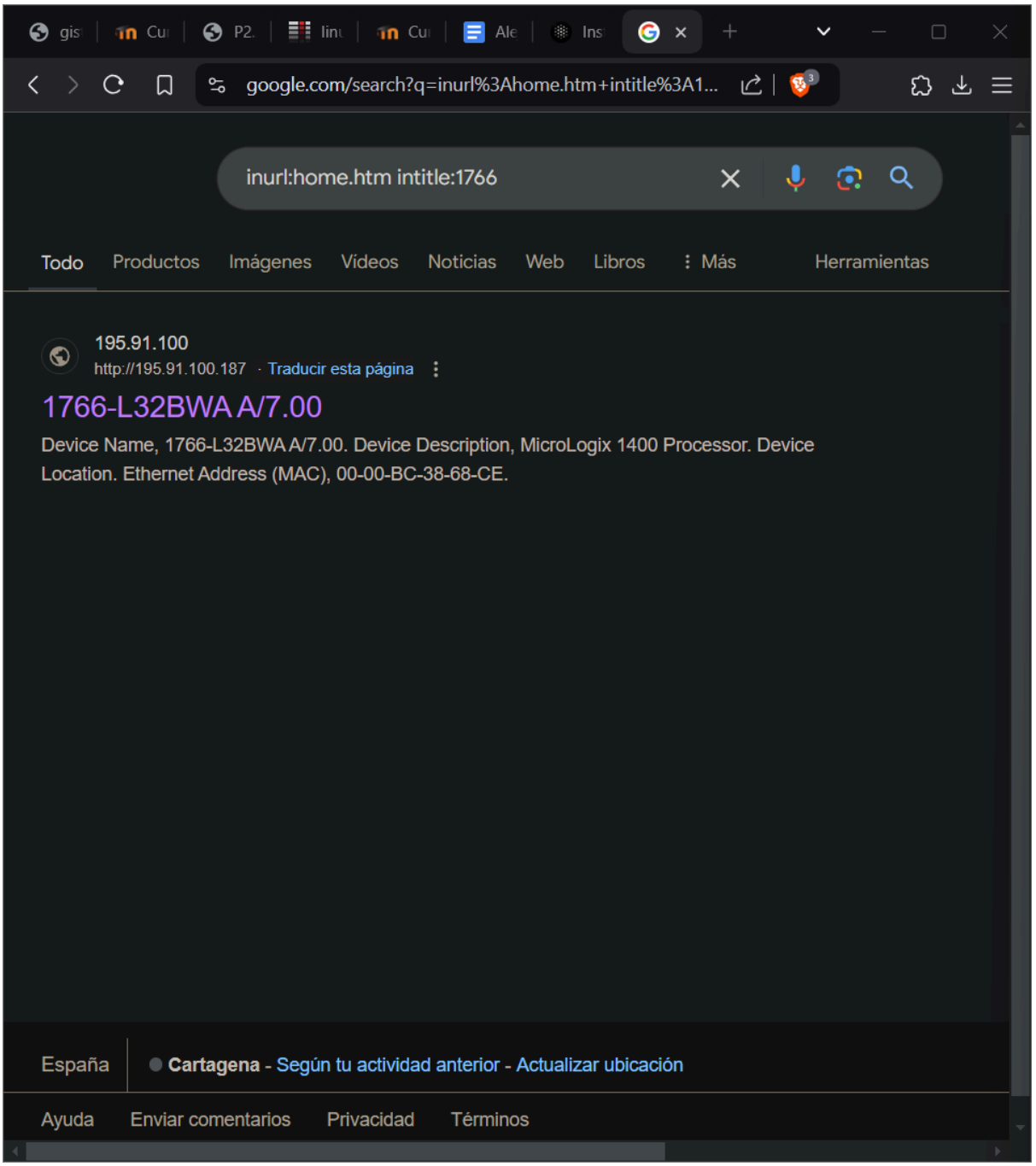
Consultas con Google Dorks

Accedemos a Exploit DB.

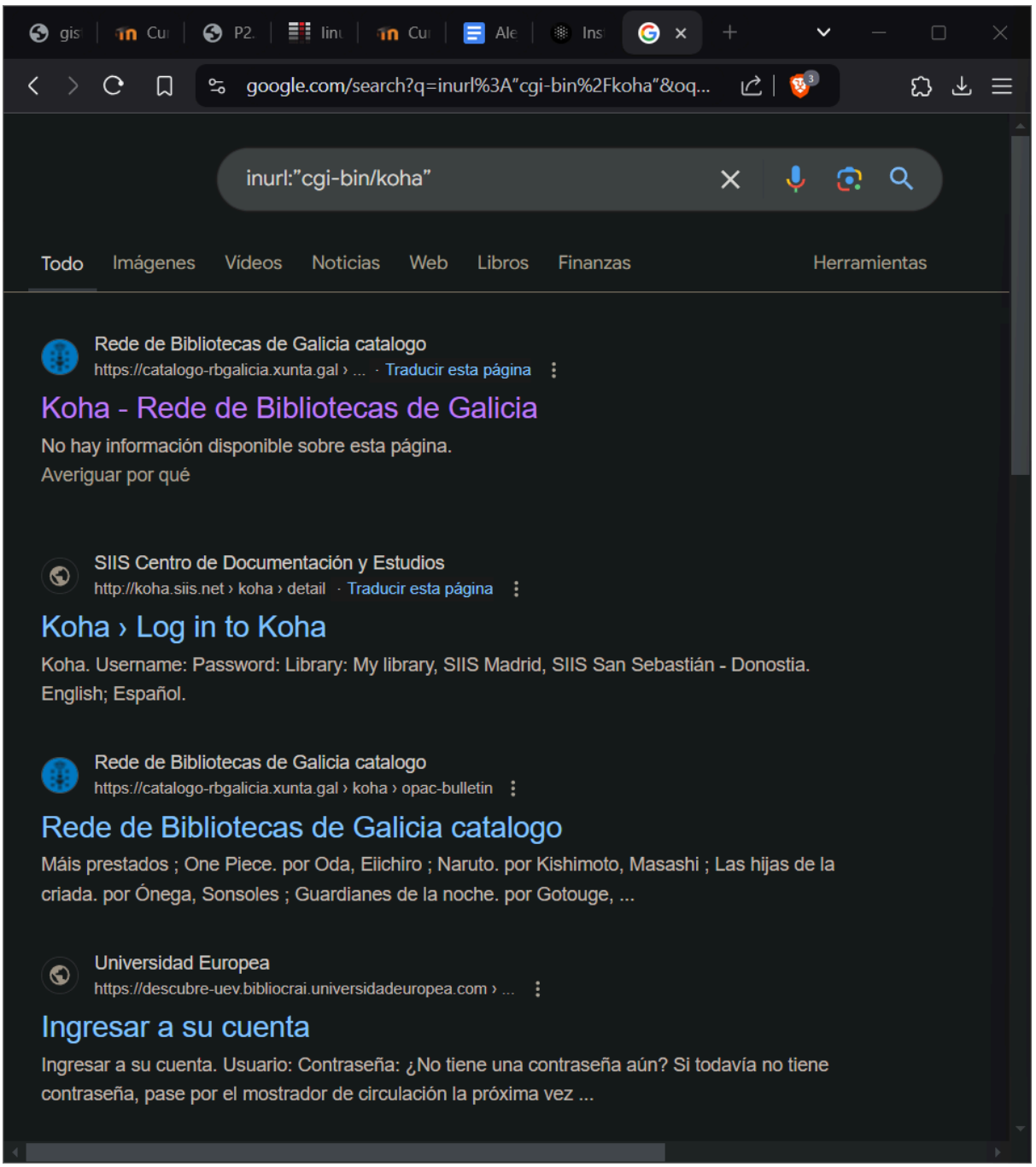
1. Dork: **site:github.com “BEGIN OPENSSH PRIVATE KEY”**
    - Búsqueda: No se encontró nada expuesto por lo menos en las primeras páginas, todo son resolución de problemas sobre el tema.



2. Dork: **inurl:home.htm intitle:1766**
    - Búsqueda: Se encuentra una sola pagina con la informacion de algun dispositivo, la MAC...



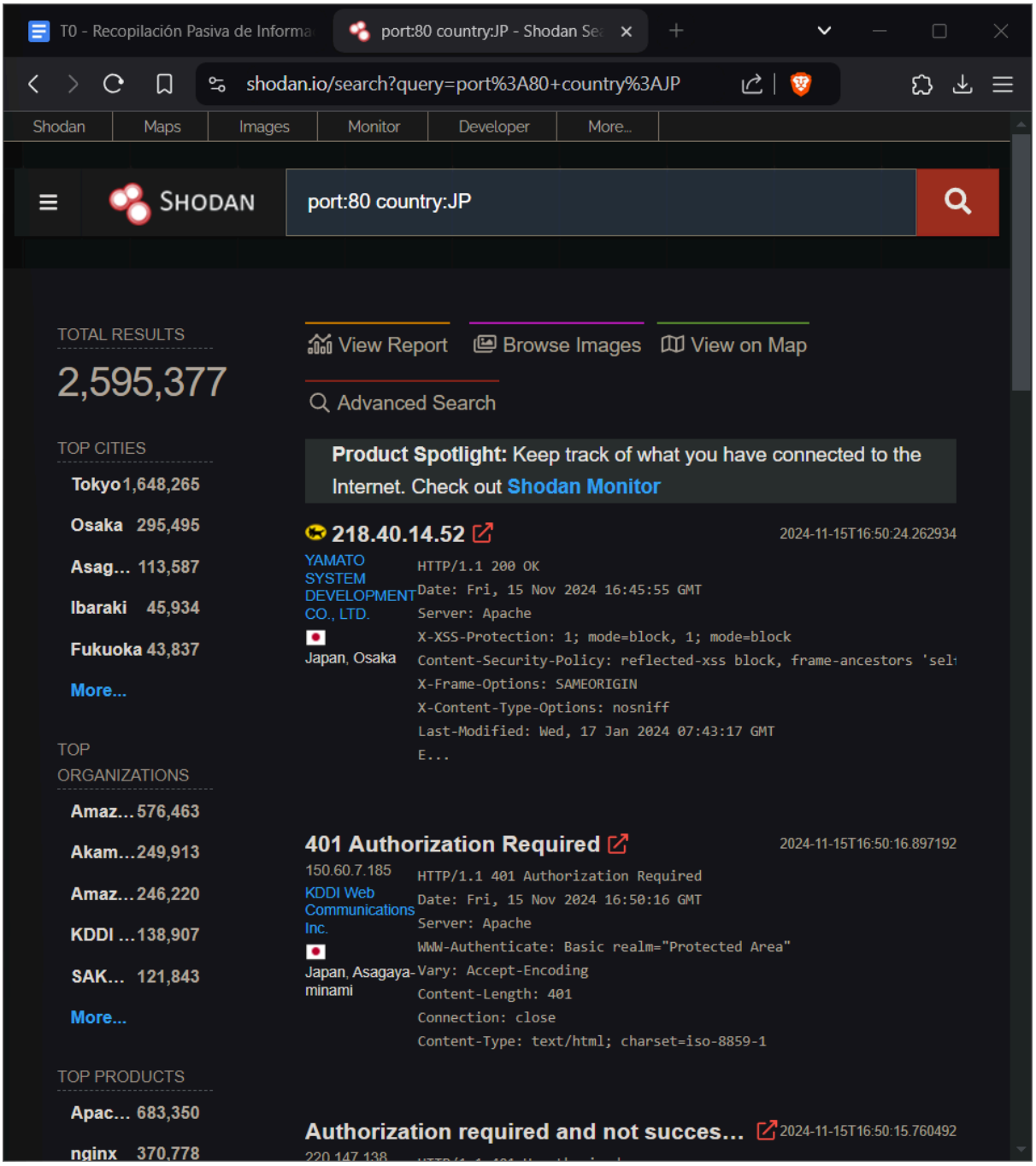
3. Dork: **inurl:”cgi-bin/koha”**
    - Búsqueda: Muestra catálogos de bibliotecas en línea que utilizan koha.



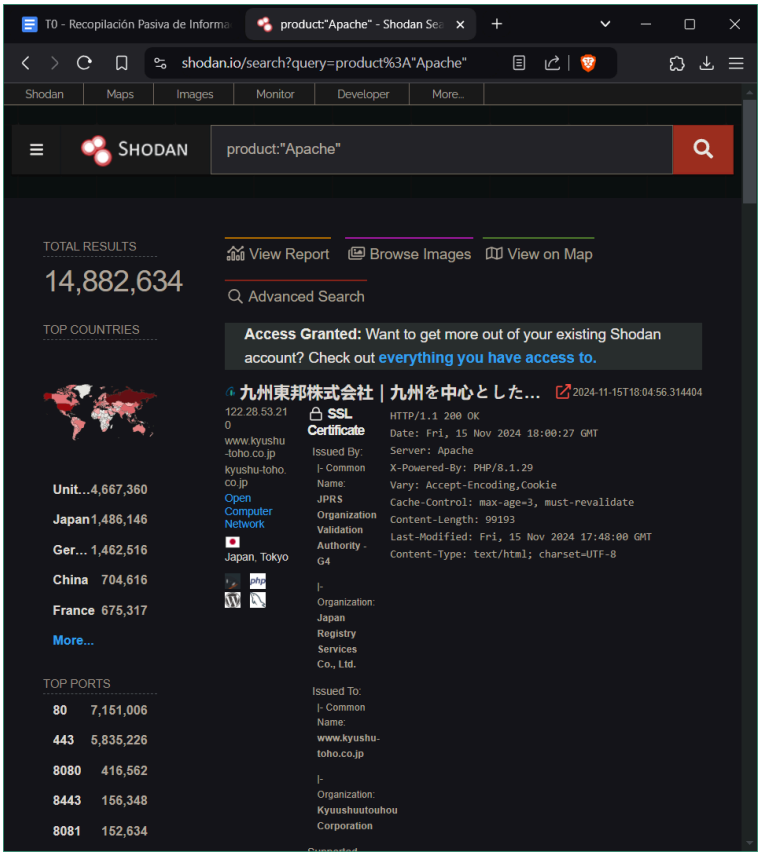
Parte 2: Exploración de Shodan

Búsquedas Avanzadas en Shodan

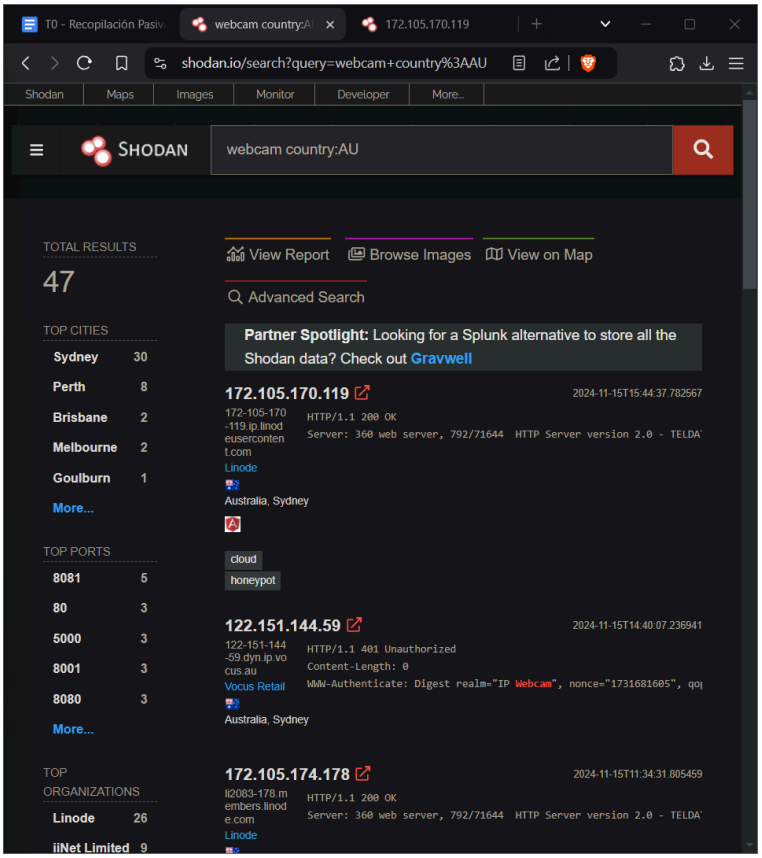
1. Búsqueda: port:80 country:JP
    - Resultados: Se encontraron millones de resultados con el puerto 80 abierto en Japón.



2. Búsqueda: product:”Apache”
    - Resultados: Busca servidores usando Apache, cerca de 15 millones en total.



3. Búsqueda: webcam country:AU
    - Resultados: Este hace una búsqueda de webcams en Australia.



Parte 3: Reflexión ética

El uso de herramientas como Google Hacking y Shodan plantea importantes consideraciones éticas y legales.

Uno de los riesgos más significativos de utilizar estas herramientas en sistemas no autorizados es la posibilidad de exponer información sensible, lo que puede resultar en violaciones de datos y daños a la reputación de la organización. Además, la recopilación de información sin permiso puede ser considerada como un acto de intrusión, que podría tener consecuencias legales graves.

En conclusión, aunque Google Hacking y Shodan son herramientas poderosas para la recopilación de información, su uso debe ser guiado por principios éticos y legales.